

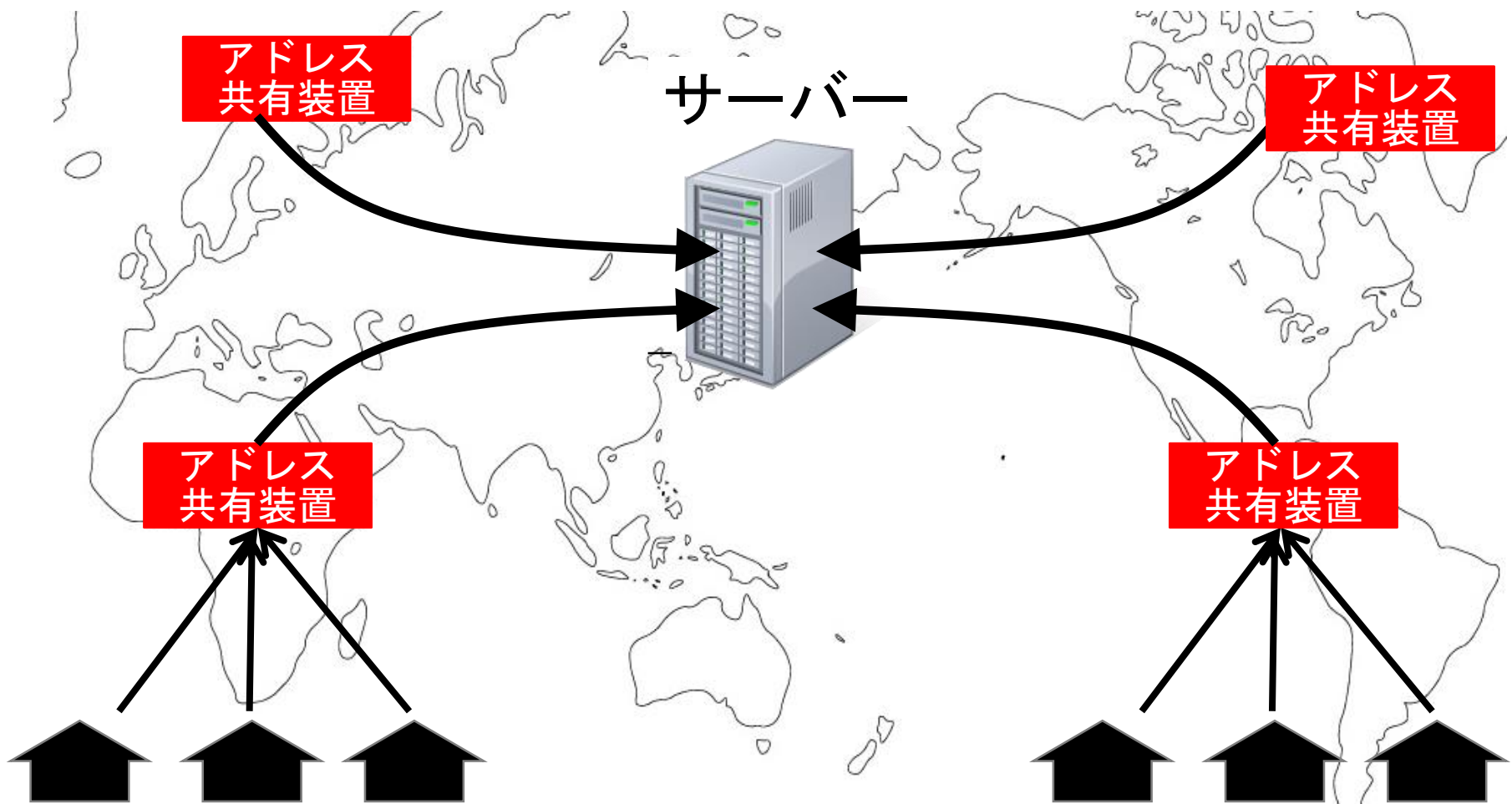
IPv4アドレス共有時の送信者特定 ～ 省令とサーバ運用 ～

2014. 7. 18

日本ネットワークイネイブラー株式会社
(JPNE)

中川あきら

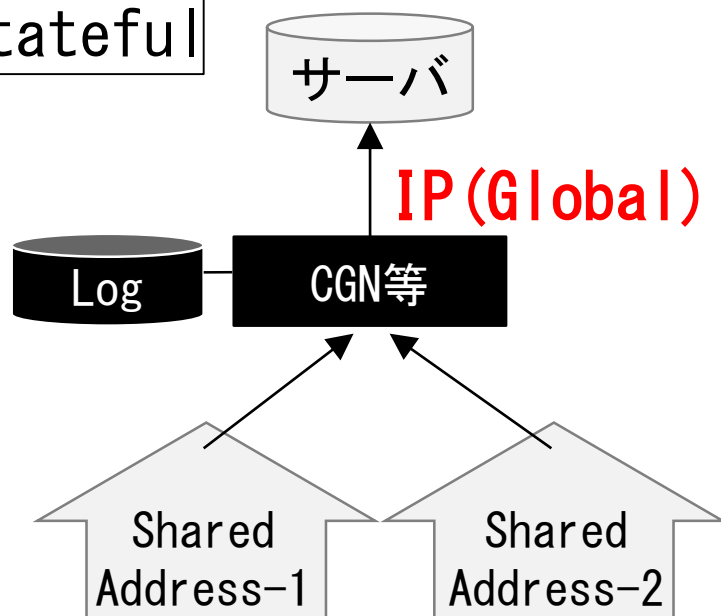
世界的にアドレス共有が始まっており、
送信者の特定が難しくなっている。



IPv4アドレス共有時の送信者特定の課題

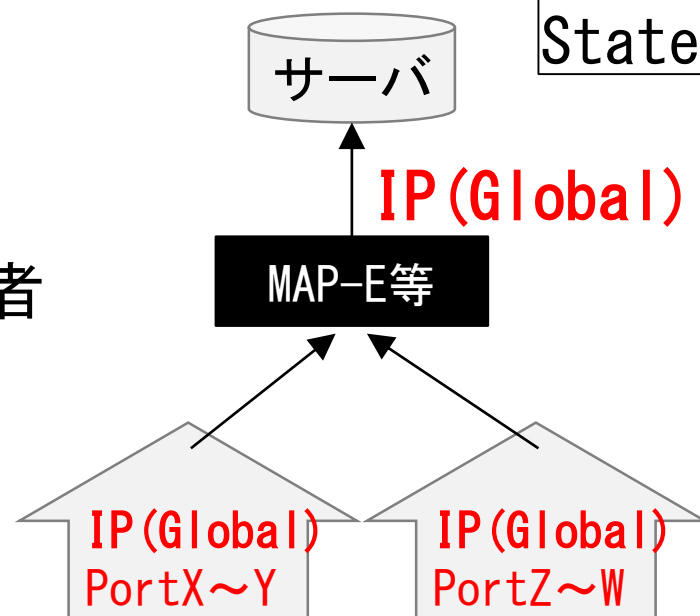
方式を問わず、送信者特定のためには
サーバ事業者はポート番号の申告が必要となる。

Stateful



NW事業者

Stateless

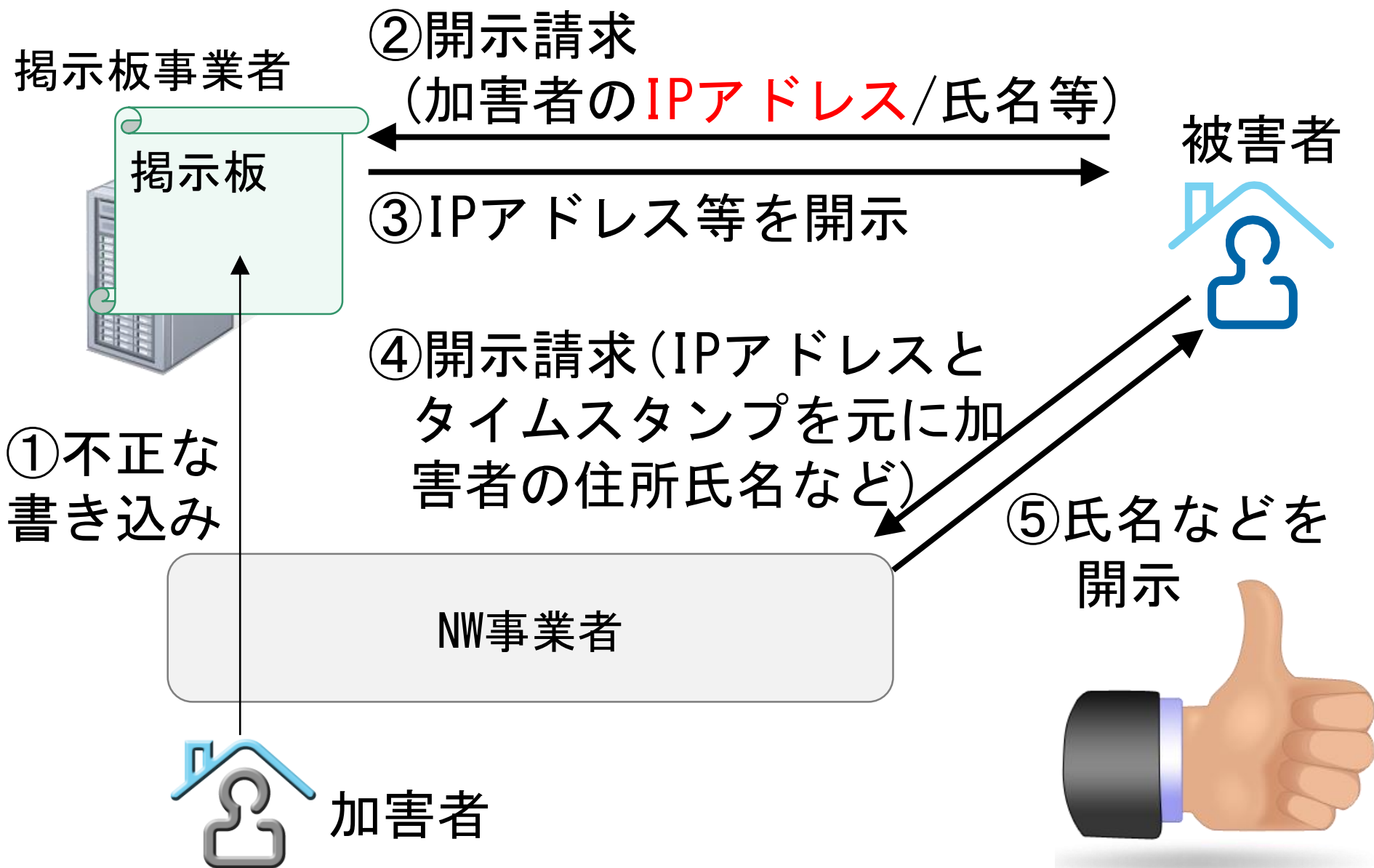


同時刻に複数からのアクセス
があると、NW事業者がLogを
取得していても、IPのみでは
送信者を特定できない。(*1)

NW事業者はセッション情報
を持っていないため、IPのみで
は送信者を特定できない。

(*1) 同時刻に複数からのアクセスが無いと考えるNW事業者も存在すると想定

従来のabuseの対応(例)

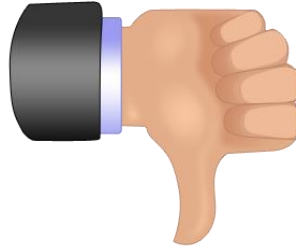


IPv4アドレス共有時のabuse対応の難しさ

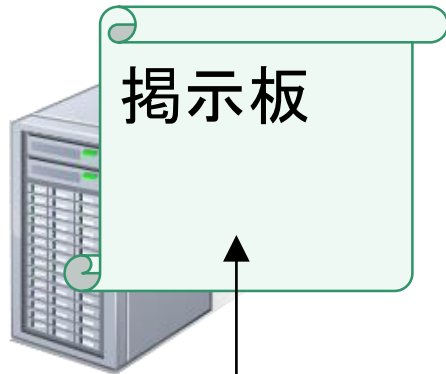
掲示板事業者

③「省令」を順守すると、
加害者のPort番号を開示
請求することができない。

被害者



掲示板



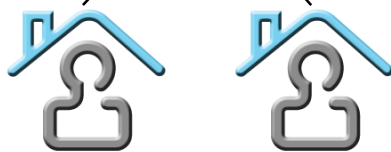
②不正な
書き込み

IPv4(共有)

アドレス
共有装置

NW事業者

①「発信者特定のためには
Port番号も必要。」



加害者

現行の省令について

被害者はポート番号を開示請求することができない。

【プロバイダ責任制限法】

被害者はプロバイダ等^(※1)に対し、発信者情報(氏名、住所その他**総務省令で定めるもの**)の開示を請求することができる。

【総務省令】(現行)

総務省令で定めるものは、発信者の：

- ・氏名・住所
- ・メールアドレス
- ・IPアドレス
- ・等

Port番号の記載無し。

【プロバイダ責任制限法】

<http://law.e-gov.go.jp/htmldata/H13/H13H0137.html>

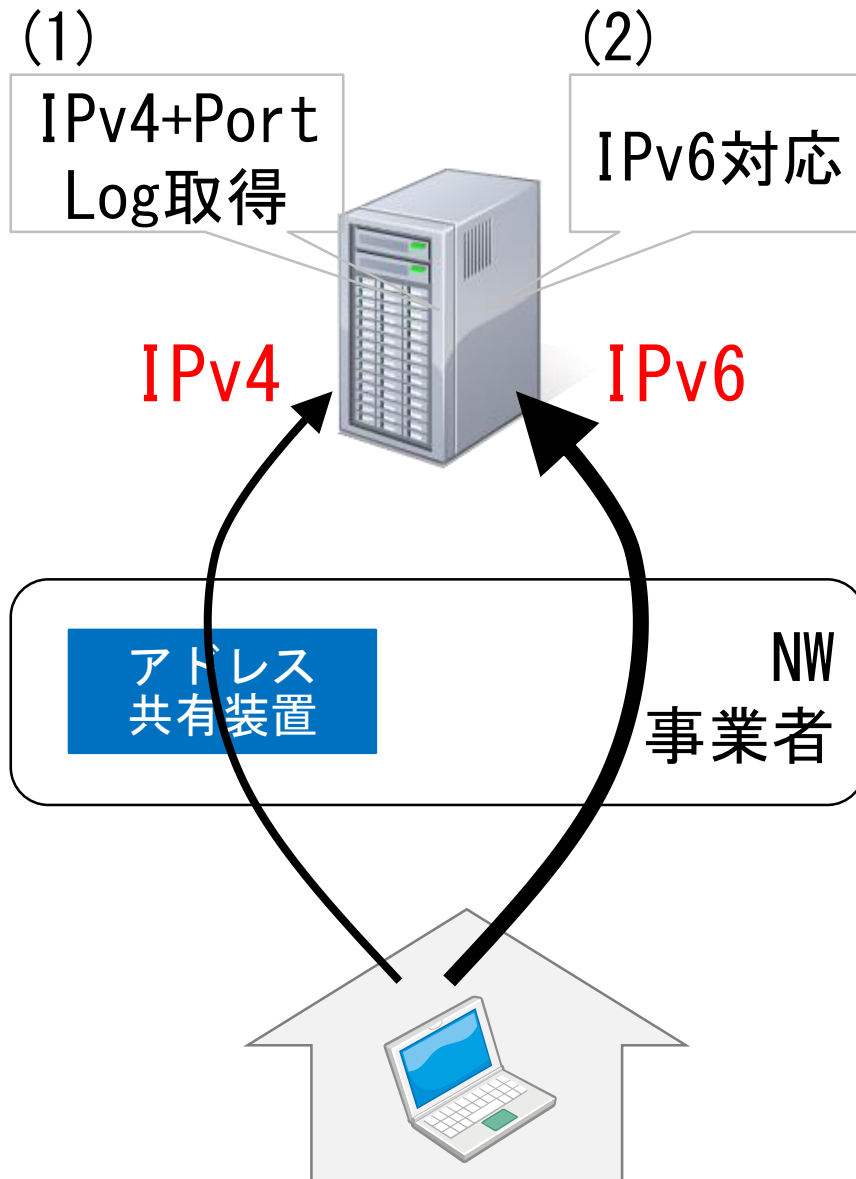
【総務省令】

<http://law.e-gov.go.jp/htmldata/H14/H14F11001000057.html>

(※1) サーバー運営事業者等を含む

今後必要となるアクションは？

今後必要となるアクション（サーバ運用面）



サーバ・F/W等の管理者は点検が必要ではないか。

(1) Port番号もLog取得できているか、又は取得するべきかどうか。

(2) IPアドレスのみで送信者を特定するために、IPv6対応して、IPv6側に多くのトラフィックを逃すべきかどうか。(*)

(*) IPv4アドレスを共有している各国のNW事業者はIPv6対応している確率が高い！

今後必要となるアクション（制度面）

総務省令の改正が必要ではないか。
総務省への働きかけも検討中。

（現行）

（略）
三 侵害情報にかかる IPアドレス
（略）
七 第四号の IPアドレス を割り当てられた電気通信設備・・・
（略）



（案）

（略）
三 侵害情報にかかる IPアドレスとPort番号（略）
七 第四号の IPアドレスとPort番号 を割り当てられた電気通信設備・・・
（略）

(参考)

RFC6302 (BCP) における推奨事項

RFC6302

Logging Recommendations for Internet-Facing Servers

Internetに接続されているサーバーで、
以下のログを取得することを推奨する。

- ソースポート番号
- 正確なタイムスタンプ (UTC推奨)
- トラnsポートプロトコル (通常 TCP or UDP)
とデスティネーションポート番号 (アプリが複数
のトラnsポートや複数のポートを使う場合)

WebサーバアプリのPortのログ取得可否

初期設定ではPort番号を取得していない傾向がある。

設定により ポート番号取得可能	ポート番号取得 非サポート
• Apache • Postfix • Sendmail • sshd	• IIS • Cyrus IMAP(*) • UW IMAP(*)

(*) ソースコード編集により可能

(注意) Load Balancer等によりIPアドレスやPort番号等が書き換えられる場合、サーバーはそれらの装置と連携してLog取得をする必要がある。

参照 I-D (2014年1月に失効しているが . . .)

<http://tools.ietf.org/html/draft-tsou-behave-natx4-log-reduction-04>



日本ネットワークイネイブラー株式会社

<http://jpne.co.jp>